

IN THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) An unauthorized access avoiding method in an intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol, the unauthorized access avoiding method in an intelligent interconnecting device comprising the steps of:

when an access from the external apparatus is authenticated through execution of the TCP/IP protocol, judging whether the access from the external apparatus is a first access,

if judged to be the first access, extracting and storing a source IP address included in a packet which is transmitted from an external apparatus ~~when an access from the external apparatus is authenticated through execution of the TCP/IP protocol;~~

judging, when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; ~~and~~

permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address; and

registering the source IP address of the external apparatus which is judged to be nonidentical in an unauthorized access IP list and notifying an authenticated

managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address.

2. – 4. (Canceled)

5. (Original) An unauthorized access avoiding method in an intelligent interconnecting device according to claim 1, further comprising the steps of:

judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, and
permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

6. - 10. (Canceled)

11. (Currently Amended) A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol is recorded, wherein the unauthorized access avoiding program comprises:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;
- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;
- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to

thereafter by the ok intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from the second step, when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step; and

a ninth step of determining the external apparatus whose source IP address is judged to be nonidentical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in the seventh step.

12. (Currently Amended) A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol is recorded, wherein the unauthorized access avoiding program comprises:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;
- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;

- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;
- a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the

source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device, when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step.

13. (Currently Amended) A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol is recorded, wherein the unauthorized access avoiding program comprises:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;
- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;
- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the

- intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;
- a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to store therein the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in the seventh step or is judged to be not within the predetermined valid period in the eighth step; and
an eleventh step of notifying a predetermined managing computer the source IP address of the external apparatus determined in the tenth step as the apparatus not to be responded to.

14. (Currently Amended) A recording medium in which a computer readable unauthorized access avoiding program executed in an intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol is recorded, wherein the unauthorized access avoiding program comprises:

- a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred;
- a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in the first step that the first access from outside has occurred;

- a third step of causing the intelligent interconnecting device to judge after the authentication processing in the second step whether or not authentication is given;
- a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in the third step that the authentication is given;
- a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from the external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in the fourth step;
- a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in the third step;
- a seventh step of causing the intelligent interconnecting device to judge whether or not the source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in the first step;
- an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in the seventh step;
- a ninth step of determining the external apparatus having the source IP address which is judged to be within the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent

interconnecting device to execute the steps beginning from the second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in the eighth step; and

a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be not within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to notify a predetermined managing computer of the source IP address of the external apparatus which is determined as the apparatus not to be responded to, when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in the seventh step or within the predetermined valid period in the eighth step.

15. (Canceled)

16. (Currently Amended) An intelligent interconnecting device connected to a LAN trunk line having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus connected to the LAN trunk line based on a TCP/IP protocol, the intelligent interconnecting device comprising:

a LAN trunk line interfacing section having an interface function with ~~[[a]]~~ the LAN trunk line;

a port interfacing section having an interface function with a terminal connected thereto;

a storage section for storing a program and data therein, and a central controlling section for controlling operations of said LAN trunk line interfacing section, said port

interfacing section, and said storage section, wherein said central controlling section executes the following steps:

to extract a source IP address included in a packet which is transmitted from an external apparatus and store it in said storage section when an access from the external apparatus is authenticated through execution of the TCP/IP protocol;

to judge, when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address; ~~and~~

to permit communication thereafter with the external apparatus having the source IP address identical with the stored transmitting end IP address only when the source IP address is judged to be identical with the stored source IP address; and

when the source IP address is judged to be nonidentical with the stored source IP address, said central controlling section registers the source IP address which is judged to be nonidentical with the stored source IP address in an unauthorized access IP list and said controlling section notifies an authenticated managing computer of the source IP address which is judged to be nonidentical with the stored source IP address.

17. - 19. (Canceled)

20. (Original) An intelligent interconnecting device according to claim 16, wherein, when the source IP address is judged to be identical with the stored source IP address, said central controlling section judges whether or not the source IP address which is judged to be identical

with the stored source IP address is within a valid period set in advance and permits communication thereafter between the external apparatus having the source IP address which is judged to be within the predetermined valid period and the intelligent interconnecting device only when it is judged to be within the valid period.

21. - 25. (Canceled)

26. (Original) A LAN system comprising an intelligent interconnecting device having a function of repeating a packet which is transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol, the intelligent interconnecting device being connected to a LAN trunk line while the plurality of computers being connected to the intelligent interconnecting device, wherein said intelligent interconnecting device is an intelligent interconnecting device according to claim 16.

27. - 34. (Canceled)